Listing of Claims

1. (Currently Amended) A method for facilitating secure transmission of an email message to anonymous recipients without divulging the identities of the anonymous recipients, comprising:

identifying recipients of the email message, wherein the recipients can include known recipients, who can be identified by examining the email message, and anonymous recipients, who cannot be identified by examining the email message;

generating a session key for the email message;

encrypting a body of the email message with the session key;

creating a recipient block for the email message that contains an entry for each recipient of the email message;

wherein each entry in the recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key, so that only a corresponding private key held by the recipient can be used to decrypt the encrypted session key;

wherein each entry additionally contains an identifier for the associated public key, but different than the associated public key, so that each recipient can determine whether the recipient possesses the corresponding private key that can decrypt the encrypted session key;

wherein identifiers for public keys belonging to known recipients are statistically unique;

wherein identifiers for public keys belonging to anonymous recipients are not statistically unique; and

sending the email message to the recipients.

2. (Original) The method of claim 1, wherein identifiers for public keys belonging to anonymous recipients provide only enough information to exclude a Large percentage of all possible corresponding private keys from being able to decrypt the body of the email message.

3. (Original) The method of claim 2, wherein an identifier for a public key is formed by creating a hash of the public key.

4. (Original) The method of claim 3, wherein an identifier for a public key belonging to an anonymous recipient is additionally modified so the identifier is not statistically unique;

whereby the identifier cannot be used to uniquely identify the anonymous recipient, and

whereby a recipient can use the identifier to exclude a large percentage of all possible corresponding public keys held by the recipient from matching the identifier.

5. (Original) The method of claim 1, further comprising, - encrypting the body of the email message, including a checksum into the body of the email message, so that a recipient can examine the checksum to verify that the correct private key was used in decrypting the email message

6. (Currently Amended) A method for facilitating secure transmission of an email message to anonymous recipients without divulging the identities of the anonymous recipients, comprising:

receiving the email message at a recipient, wherein the email message includes,

a message body that has been encrypted with a session key,

a recipient block that contains an entry for each recipient of the email message,

wherein each entry in the recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key,

wherein each entry additionally contains an identifier for the associated public key, but different than the associated public key,

wherein identifiers for public keys belonging to known recipients are statistically unique, and

wherein identifiers for public keys belonging to anonymous recipients are not statistically unique;

attempting to match a candidate public key held by the recipient with key identifier in the recipient block;

if the candidate public key matches a key identifier,

decrypting the associated encrypted session key using an associated private key to restore the session key,

decrypting the message body using the session key, and

examining a checksum in the message body to verify that message body was correctly decrypted.

7. (Original) The method of claim 6, wherein identifiers for public keys belonging to anonymous recipients provide only enough information to exclude a large percentage of all possible corresponding private keys from being able to decrypt the message body of the email message.

8. (Original) The method of claim 7, wherein an identifier for a public key is formed by creating a hash of the public key.

9. (Original) The method of claim 8, wherein an identifier for a public key belonging to an anonymous recipient is additionally modified so the identifier is not statistically unique;

whereby the identifier cannot be used to uniquely identify the anonymous recipient; and

whereby a recipient can use the identifier to exclude a large percentage of all possible public keys belonging to the recipient from matching the identifier.

10. (Currently Amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for facilitating secure transmission of an email message to anonymous recipients without divulging the identities of the anonymous recipients, the method comprising:

identifying recipients of the email message, wherein the recipients can include known recipients, who can be identified by examining the email message, and anonymous recipients, who cannot be identified by examining the email message;

generating a session key for the email message;

encrypting a body of the email message with the session key;

creating a recipient block for the email message that contains an entry for each recipient of the email message;

wherein each entry in the recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key, so that only a

corresponding private key held by the recipient can be used to decrypt the encrypted session key;

wherein each entry additionally contains an identifier for the public key, but different than the associated public key, so that each recipient can determine whether the recipient possesses the corresponding private key that can decrypt the encrypted session key;

wherein identifiers for public keys belonging to known recipients are statistically unique;

wherein identifiers for public keys belonging to anonymous recipients are not statistically unique; and

sending the email message to the recipients.

11. (Original) The computer-readable storage medium of claim 10, wherein identifiers for public keys belonging to anonymous recipients provide only enough information to exclude a large percentage of all possible corresponding private keys from being able to decrypt the body of the email message.

12. (Original) The computer-readable storage medium of claim 11, wherein an identifier for a public key is formed by creating a hash of the public key.

13. (Original) The computer-readable storage medium of claim 12, wherein an identifier for a public key belonging to an anonymous recipient is additionally modified so the identifier is not statistically unique;

whereby the identifier cannot be used to uniquely identify the anonymous recipient; and

whereby a recipient can use the identifier to exclude a large percentage of all possible public keys belonging to the recipient from matching the identifier.

14. (Original) The computer-readable storage medium of claim 10, wherein prior to encrypting the body of the email message, the method further comprises including a checksum into the body of the email message, so that a recipient can examine the checksum to verify that the correct private key was used in decrypting the email message.

15. (Currently Amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for facilitating secure transmission of an email message to anonymous recipients without divulging the identities of the anonymous recipients, the method comprising:

receiving the email message at a recipient, wherein the email message includes,

a message body that has been encrypted with a session key,

a recipient block that contains an entry for each recipient of the email message,

wherein each entry in the recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key,

wherein each entry additionally contains an identifier for the associated public key, but different than the associated public key,

wherein identifiers for public keys belonging to known recipients are statistically unique, and

wherein identifiers for public keys belonging to anonymous recipients are not statistically unique;

attempting to match a candidate public key held by the recipient with key identifier in the recipient block;

if the candidate public key matches a key identifier,

decrypting the associated encrypted session key using an associated private key to restore the session key,

decrypting the message body using the session key, and

examining a checksum in the message body to verify that message body was correctly decrypted.

16. (Original) The computer-readable storage medium of claim 15, wherein identifiers for public keys belonging to anonymous recipients provide only enough information to exclude a large percentage of all possible corresponding private keys from being able to decrypt the message body of the email message.

17. (Original) The computer-readable storage medium of claim 16, wherein an identifier for a public key is formed by creating a hash of the public key.

18. (Original) The computer-readable storage medium of claim 17, wherein an identifier for a public key belonging to an anonymous recipient is additionally modified so the identifier is not statistically unique;

whereby the identifier cannot be used to uniquely identify the anonymous recipient; and

whereby a recipient can use the identifier to exclude a large percentage of all possible public keys belonging to the recipient from matching the identifier.

19. (Currently Amended) An apparatus that facilitates secure transmission of an email message to anonymous recipients without divulging the identities of the anonymous recipients, comprising:

an identifying mechanism that is configured to identify recipients of the email message, wherein the recipients can include known recipients, who can be identified by examining the email message, and anonymous recipients, who cannot be identified by examining the email message;

a key generation mechanism that is configured to generate a session key for the email message;

an encryption mechanism that is configured to encrypt a body of the email message with the session key;

a recipient block creation mechanism that is configured to create a recipient block for the email message that contains an entry for each recipient of the email message;

wherein each entry in the recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key, so that only a corresponding private key held by the recipient can be used to decrypt the encrypted session key;

wherein each entry additionally contains an identifier for the associated public key, but different than the associated public key, so that each recipient can determine whether the recipient possesses the corresponding private key that can decrypt the encrypted session key;

wherein identifiers for public keys belonging to known recipients are statistically unique;

wherein identifiers for public keys belonging to anonymous recipients are not statistically unique; and

a sending mechanism that is configured to send the email message to the recipients.

20. (Original) The apparatus of claim 19, wherein identifiers for public keys belonging to anonymous recipients provide only enough information to exclude a large percentage of all possible corresponding public keys from being able to decrypt the body of the email message.

21. (Original) The apparatus of claim 20, wherein an identifier for a public key is a hash of the public key.

22. (Original) The apparatus of claim 21, wherein the recipient block creation mechanism is additionally configured to modify an identifier for a public key belonging to an anonymous recipient so the identifier is not statistically unique;

whereby the identifier cannot be used to uniquely identify the anonymous recipient; and

whereby a recipient can use the identifier to exclude a large percentage of all possible public keys held by the recipient from matching the identifier.

23. (Original) The apparatus of claim 19, further comprising a checksum mechanism that, wherein prior to encrypting the body of the email message, the checksum mechanism is configured to include a checksum into the body of the email message, so that a recipient can examine the checksum to verify that the correct private key was used in decrypting the email message.

24. (Currently Amended) An apparatus that facilitates secure transmission of an email message to anonymous recipients without divulging the identities of the anonymous recipients, comprising:

a receiving mechanism that is configured to receive the email message at a recipient, wherein the email message includes,

a message body that has been encrypted with a session key,

a recipient block that contains an entry for each recipient of the email message,

wherein each entry in the recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key,

wherein each entry additionally contains an identifier for the associated public key, but different than the associated public key,

wherein identifiers for public keys belonging to known recipients are statistically unique, and

wherein identifiers for public keys belonging to anonymous recipients are not statistically unique;

a matching mechanism that is configured to attempt to match a candidate public key belonging to the recipient with key identifier in the recipient block;

a decryption mechanism, wherein if the candidate public key matches a key identifier, the decryption mechanism is configured to,

decrypt the associated encrypted session key using a corresponding private key to restore the session key,

decrypt the message body using the session key, and to

examine a checksum in the message body to verify that message body was correctly decrypted.

25. (Original) The apparatus of claim 24, wherein identifiers for public keys belonging to anonymous recipients provide only enough information to exclude a large percentage of all possible corresponding private keys from being able to decrypt the message body of the email message.

26. (Original) The apparatus of claim 25, wherein an identifier for a public key is a hash of the public key.

27. (Original) The apparatus of claim 26, wherein an identifier for a public key belonging to an anonymous recipient is additionally modified so the identifier is not statistically unique;

whereby the identifier cannot be used to uniquely identify the anonymous recipient; and

whereby a recipient can use the identifier to exclude a large percentage of all possible public keys belonging to the recipient from matching the identifier.